# GALOIS THEORY
# Worksheet 3



**Q 1** (†)**.** Let $K$ be a field of characteristic 0 containing an element $\omega \in K$ with

$$\omega^2 + \omega + 1 = 0\,.$$

(For example you can take $K = \mathbb{Q}(\omega)$ where $\omega = \exp \frac{2\pi \mathrm{i}}{3}$.) In this question we carve a trick-free path to the formula for the solutions of the equation

$$X^3 + 3pX + 2q = 0 \qquad (\dagger)$$

(where $p$, $q \in K$) that only involves taking radicals (i.e., $\sqrt[n]{\ }$ of something).

We assume that $K \subset L$ is the splitting field of the polynomial of Equation (†) and we denote by $\alpha_1$, $\alpha_2$, $\alpha_3 \in L$ the three roots. (You can already prove that such a field extension exists but I don't care that you do this here.)

We know that the Galois group $G$ permutes the three roots.

(a) Write the action of the cyclic permutation $\sigma = (123)$ on the elements[1]

$$u = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3, \quad v = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3\,.$$

and conclude that $\sigma(u) = \omega^2 u$ and $\sigma(v) = \omega v$.[2]

(b) Find a formula expressing the three roots $\alpha_1$, $\alpha_2$, $\alpha_3$ in terms of $u$ and $v$.

[*Hint*: $\alpha_1 + \alpha_2 + \alpha_3 = 0$.]

(c) Consider the transposition $\tau = (23)$: show that $\tau(u) = v$ and $\tau(v) = u$, and hence argue that $u^3 + v^3$ and $u^3v^3$ are fixed by all of $\mathfrak{S}_3$ — and hence by all of $G$, irrespective of what $G$ is. In other words, it follows from the Galois Correspondence that $u^3 + v^3$ and $u^3v^3 \in K$: show that this is indeed the case by finding explicit formulas for these quantities. Thus write down an explicit quadratic polynomial in $K[X]$ of which $u^3$, $v^3$ are the two roots. Solve the quadratic equation, and combine with (b) to derive the cubic formula.

**Q 2.** In this question, if $\alpha \in \mathbb{R}_{>0}$ and $n \in \mathbb{Z}_{>0}$ then by $\alpha^{1/n}$ or $\sqrt[n]{\alpha}$ I mean the unique positive real number $\beta$ with $\beta^n = \alpha$. (This removes ambiguities about a general complex number having $n$ complex roots in this question).

---

[1] Why is it not a "trick" to write down such elements? Consider the permutation matrix acting cyclically on the standard basis of $\mathbb{R}^3$. This is a rotation! Figure out the Jordan normal form and write down the change of basis matrix to a basis of eigenvectors over $\mathbb{C}$.

[2] Whether or not there is an element of $G$ that acts as $\sigma$ on the three roots is not relevant at this point. Such an element may or may not exist.

(i) Set $\gamma = (1+\sqrt{3})^{1/3}$. Prove that $\gamma$ is *algebraic* over $\mathbb{Q}$.[3] What is its degree over $\mathbb{Q}$? What is its degree over $\mathbb{Q}(\sqrt{3})$?

(ii) Set $\delta = (10+6\sqrt{3})^{1/3}$. Prove that $\delta$ is algebraic over $\mathbb{Q}$. What is its degree over $\mathbb{Q}$? What is its degree over $\mathbb{Q}(\sqrt{2})$?

**Q 3.** Factor the following polynomials in $\mathbb{Q}[X]$ into irreducible ones, giving proofs that your factors really are irreducible.

(i) $X^3 - 8$;

(ii) $X^{1000} - 6$;

(iii) $X^4 + 4$;

(iv) $2X^3 + 5X^2 + 5X + 3$;

(v) $X^5 + 6X^2 - 9X + 12$;

(vi) $X^{73} - 1$;

(vii) $X^{73} + 1$;

(viii) $X^{12} - 1$.

**Q 4.** Prove that if $\alpha = 2^{1/10}$ then $\mathbb{Q}(\alpha)$ has a basis $\{1, \alpha, \alpha^2, \ldots, \alpha^9\}$.

[3] Let $K \subset L$ be a field extension, not necessarily finite. By definition, an element $z \in L$ is algebraic over $K$ if it is the root of a polynomial with coefficients in $K$. Its degree is by definition the degree of the minimal polynomial.